Guía de Seguridad de las TIC
CCN-STIC 1119

Procedimiento de Empleo Seguro
iMC MagicBox

Marzo 2026

Edita:

centro criptológico nacional

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.04.06 08:28:12 +02'00'

Fecha de Edición: Marzo de 2026

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1 INTRODUCCIÓN 3
2 OBJETO Y ALCANCE 4
3 ORGANIZACIÓN DEL DOCUMENTO 5
4 FASE PREVIA A LA INSTALACIÓN 6
4.1 ENTREGA SEGURA DEL PRODUCTO 6
4.1.1 REVISIÓN DE FIRMWARE 6
4.1.2 REVISIÓN DE HARDWARE 6
4.2 ENTORNO DE INSTALACIÓN SEGURO 7
4.3 REGISTRO Y LICENCIAS 7
4.4 CONSIDERACIONES PREVIAS 8
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 9
5 FASE DE INSTALACIÓN 10
5.1 PREPARACIÓN PARA LA INSTALACIÓN 10
5.2 INSTALACIÓN 10
5.3 INSTALACIÓN DE COMPONENTES ADICIONALES 10
6 FASE DE CONFIGURACIÓN 11
6.1 MODO DE OPERACIÓN SEGURO 11
6.2 AUTENTICACIÓN 11
6.2.1 AUTENTICACIÓN DE ADMINISTRADORES 11
6.2.2 AUTENTICACIÓN DE DISPOSITIVOS GESTIONADOS 12
6.3 ADMINISTRACIÓN DEL PRODUCTO 12
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 12
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 13
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 17
6.5 GESTIÓN DE CERTIFICADOS 17
6.6 SERVIDORES DE AUTENTICACIÓN 19
6.6.1 CONFIGURACIÓN CON RADIUS 19
6.6.2 CONFIGURACIÓN CON LDAP 20
6.6.3 CONFIGURACIÓN CON TACACS 22
6.7 SINCRONIZACIÓN 22
6.7.1 CONFIGURACIÓN NTP 22
6.8 ACTUALIZACIONES 23
6.9 AUTO-CHEQUEOS 24
6.10 ALTA DISPONIBILIDAD 24
6.11 AUDITORÍA 25
6.11.1 REGISTRO DE EVENTOS 25
6.11.2 ALMACENAMIENTO LOCAL 26
6.11.3 REENVÍO DE EVENTOS 26
6.12 BACKUP 26
7 REFERENCIAS 28
8 ABREVIATURAS 29

1 INTRODUCCIÓN

1. El producto **H3C Intelligent Management Center (iMC)** es una plataforma de gestión de red y seguridad destinada a organizaciones con infraestructuras complejas y distribuidas. Está basada en una arquitectura modular que permite integrar distintos componentes y centralizar en un único entorno las tareas de supervisión, control y operación de la red.
2. En términos generales, iMC funciona como un punto central de administración que ofrece una visión unificada de los elementos de la red, tanto físicos como virtuales, sin importar su tamaño, fabricante o ubicación. La plataforma permite disponer de un inventario actualizado, gestionar configuraciones de forma uniforme, monitorizar parámetros de rendimiento y generar alarmas centralizadas para el seguimiento de incidentes.
3. La solución cubre la gestión de la red desde el acceso de usuarios y dispositivos hasta la supervisión de servicios de negocio. Incluye mecanismos para la aplicación de políticas de seguridad, la automatización de tareas, la consistencia en cambios de configuración y el control de acceso de usuarios y dispositivos a los recursos de red.
4. Las funciones principales son:
    - **Gestión de recursos de red:** descubrimiento automático, vistas de dispositivos, topologías e inventario.
    - **Gestión de configuración y cambios:** plantillas, backups y cumplimiento de políticas.
    - **Gestión de fallos y rendimiento:** monitorización en tiempo real, alarmas, paneles de rendimiento y análisis de tráfico.
    - **Gestión de seguridad:** control de accesos, auditoría de comportamiento, políticas de seguridad y defensa de admisión de endpoints (EAD).
    - **Gestión de servicios y aplicaciones:** visibilidad del estado de servicios empresariales y soporte para aplicaciones de terceros.

2 OBJETO Y ALCANCE

5. El objeto de este documento es establecer el procedimiento de empleo seguro de los equipos **iMC MagicBox** del fabricante H3C para las versiones y equipos definidos en el catálogo de productos CPSTIC de acuerdo a la configuración cualificada para ENS.

6. El producto **iMC MagicBox** ha sido cualificado en el catálogo CPSTIC para categoría ENS ALTO en las familias “B.3 Herramientas de gestión de red” y “A.1 Dispositivos de Control de Acceso a Red”. Se debe comprobar el estado de cualificación (que esta se mantiene) y que la versión de este documento es la más actualizada.

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración y operación del producto, para lograr una configuración segura.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. iMC está disponible tanto como un dispositivo de red físico como en formato de dispositivo virtual (software). Si se dispone de la versión de dispositivo físico aplican las dos subsecciones de este apartado. En caso de contar con un "dispositivo virtual" solo es de aplicación la subsección 4.1.1 REVISIÓN DE FIRMWARE.

4.1.1 REVISIÓN DE FIRMWARE

8. La imagen del software tiene una firma digital. Cuando el dispositivo arranca, la firma digital se verifica automáticamente, si falla, el producto no continuará con el arranque (principio de diseño *fail-safe*) y mostrará un mensaje de error.

4.1.2 EN CASO DE QUE DURANTE UN ARRANQUE SE MUESTRE UN MENSAJE DE ERROR INDICANDO QUE EL FIRMWARE NO ES VÁLIDO EL ADMINISTRADOR DEBE DESCARGAR UNA VERSIÓN VALIDA DEL FIRMWARE, ABRIR LA INTERFAZ DE "DEPLOYMENT MANAGEMENT" E INICIAR EL PROCEDIMIENTO DE ACTUALIZACIÓN, TAL Y COMO SE INDICA EN LA SECCIÓN 6.7.1 CONFIGURACIÓN NTP

9. Esta sección describe el procedimiento para configurar la sincronización horaria mediante NTP (Network Time Protocol) en H3C iMC MagicBox. Mantener la hora del sistema correctamente sincronizada es esencial para el correcto funcionamiento del equipo (ej. análisis de logs).

10. La configuración de la sincronización horaria mediante NTP se debe seguir el siguiente procedimiento:

    a) Inicie sesión en el sistema utilizando una cuenta de administración.

    b) Abra el fichero de configuración de NTP con el siguiente comando:

```
sudo vi /etc/ntp.conf
```

    c) En el fichero de configuración, añada o modifique las siguientes líneas para definir el/los servidor(es) NTP:

```
server <IP_O_HOSTNAME_NTP> iburst
```

    d) Compruebe la zona horaria actual del sistema:

```
Timedatectl
```

    e) Si es necesario, configure la zona horaria correcta:

```
sudo timedatectl set-timezone <location>
```

    f) Inicie el servicio NTP:

```
sudo systemctl start ntpd
```

    g) Configure el servicio para que se inicie automáticamente tras un reinicio del sistema:

```
sudo systemctl enable ntpd
```

    h) Compruebe que el servicio NTP se encuentra en ejecución correctamente:

```
sudo systemctl status ntpd
```

i) Tras unos minutos, verifique que el sistema se ha sincronizado con los servidores NTP configurados. Si la sincronización es correcta, los servidores NTP remotos aparecerán listados con estado alcanzable:

```
ntpq -p
```

j) Si el cortafuegos del sistema está activo, permita el tráfico NTP:

```
sudo firewall-cmd --add-service=ntp --permanent
sudo firewall-cmd –reload
```

11. La opción `iburst` (apartado "c)") permite una sincronización inicial más rápida al acelerar el intercambio inicial de paquetes con los servidores NTP. Asimismo, se recomienda configurar **al menos dos servidores NTP** con el fin de proporcionar redundancia y mejorar la disponibilidad y fiabilidad de la sincronización horaria.
12. ACTUALIZACIONES.
13. Cada vez que se realice una actualización del software, la firma digital de la nueva imagen será comprobada por el dispositivo. Para más información sobre el proceso de comprobación de firmware ver la sección 6.9 AUTO-CHEQUEOS.

4.1.3 REVISIÓN DE HARDWARE

14. Para asegurarse que el producto no ha sido modificado durante su transporte, revisar el paquete que se entrega de la siguiente manera:
15. **Revisión Exterior:**
    - Comprobar que el embalaje exterior está en buenas condiciones.
    - Comprobar la cinta de embalar y etiquetas del embalaje de cartón exterior.
    - Comprobar el sellado de la bolsa plástica que se encuentra dentro del embalaje de cartón.
16. Si alguna de estas comprobaciones no es satisfactoria, será necesario ponerse en contacto con el fabricante a la mayor brevedad posible.
17. **Comprobación de contenido:**
18. Revisar con la lista de elementos el contenido del paquete. Si hay alguna discrepancia en cuanto al tipo o número de elementos, el producto será necesario ponerse en contacto con el fabricante a la mayor brevedad posible.
19. **Inspección visual del contenido:**
20. Inspeccionar defectos en el chasis, conexiones dañadas, otro tipo de daños externos y etiquetas ilegibles. Si alguna superficie o material tiene daños, será necesario ponerse en contacto con el fabricante a la mayor brevedad posible.

4.2 ENTORNO DE INSTALACIÓN SEGURO

21. El producto se debe desplegar en un entorno físico protegido, donde solo pueda acceder el personal expresamente autorizado por la organización y que disponga de las medidas de seguridad adecuadas. Se debe garantizar que el producto se encuentra protegido por su

entrono operacional y no está sujeto a ataques físicos que pudiesen comprometer su seguridad o interferir en su correcta operación.

22. El sistema operativo donde se instale el producto debe estar actualizado y administrado de forma confiable. El usuario administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la red de comunicaciones. Por ello, se asume que dicha persona estará suficientemente capacitada y carecerá de cualquier intención dañina al administrar estos dispositivos.
23. Los requisitos del entorno de instalación se pueden encontrar en la sección 4.4 CONSIDERACIONES PREVIAS.

4.3 REGISTRO Y LICENCIAS

24. El **registro del producto iMC** se realiza tras la instalación de la plataforma. Una vez desplegado el sistema y accedido a la consola web por primera vez, el administrador debe cargar el archivo de licencia suministrado por H3C. Para obtener el fichero de licencia se deben seguir los pasos indicados en la sección “Registering and installing a license” de [REF5].
25. Este registro inicial activa el producto y valida el número de dispositivos o usuarios que podrán gestionarse en función del tipo de licencia adquirida (ver [REF5] para más información). Sin este paso, el sistema se ejecuta en un modo restringido, limitando su capacidad hasta que se registre correctamente.
26. En la **plataforma iMC**, las licencias se asocian al número de dispositivos gestionados. Cada equipo de red que se incorpora al inventario de iMC —ya sea un switch, un router, un firewall o un punto de acceso— consume un nodo de licencia. El sistema mantiene siempre disponible la información sobre cuántos nodos han sido licenciados y cuántos están en uso, de modo que cuando se intenta añadir un dispositivo adicional que exceda la capacidad permitida, iMC lo notifica y bloquea la operación hasta que se amplíe la licencia. Esta ampliación se realiza cargando un nuevo archivo de licencia desde la propia consola web, en la sección de configuración del sistema, lo que actualiza automáticamente el número de nodos disponibles.
27. El módulo **User Access Manager (UAM)** utiliza un modelo diferente. Aquí el licenciamiento no depende de los dispositivos, sino de los **usuarios concurrentes** que se autentican en la red. UAM se gestiona mediante la denominada **EIA license (Enterprise Intelligent Access license)**, que fija un número máximo de usuarios en línea de forma simultánea. El sistema controla en todo momento tanto el número total permitido por la licencia como los usuarios actualmente conectados y el máximo histórico alcanzado. Además, cuando el consumo llega al 95 % de la capacidad licenciada, UAM genera una alarma crítica para advertir a los administradores de que se está cerca del límite.
28. En iMC la información sobre el número de licencias se puede consultar directamente desde la propia interfaz web, aunque la forma de hacerlo varía ligeramente según se trate de la **plataforma iMC** o del **módulo UAM**:
    - En la **plataforma iMC (Enterprise/Standard)**, el número de licencias disponibles y utilizadas se visualiza desde el menú **Help > About** en la parte superior derecha de la consola. En esta ventana se muestran los detalles de la instalación, incluido el número total de nodos gestionables, los ya consumidos y los que aún están libres.

- En **iMC UAM (User Access Manager)**, la información de licencias se presenta como parte de la gestión de la **EIA license**. El sistema muestra tres valores clave:
  - **Total License Number** (número máximo de usuarios concurrentes permitidos por licencia).
  - **EIA Used** (usuarios concurrentes actualmente conectados).
  - **Max. History License Usage** (máximo histórico alcanzado). Además, si se supera el 95 % del número de usuarios concurrentes autorizados, UAM genera automáticamente una alarma crítica.

29. Para más información sobre el licenciamiento ver la sección “Adding devices in iMC” en [REF1] y “EIA license” en [REF2].

4.4 CONSIDERACIONES PREVIAS

30. En el esquema de despliegue distribuido, los servidores iMC incluyen servidores conductores y servidores miembros.
31. El servidor conductor es el centro de gestión del sistema iMC, responsable de coordinar con todos los servidores miembro para completar colectivamente las tareas de administración.
32. Un servidor miembro se encarga de tareas de gestión específicas, como los servicios de análisis de tráfico para NTA (Network Traffic Analyzer) y los servicios de portal para UAM.
33. En el esquema de despliegue distribuido, primero instale todos los componentes en el servidor conductor y, posteriormente, en los servidores miembro según sea necesario. El servidor conductor proporciona un portal web unificado que permite a los usuarios acceder a todas las funciones de gestión de iMC, simplemente accediendo al servidor conductor. Para más información sobre el despliegue distribuido ver la sección “Deployment restrictions and guidelines” de [REF4].
34. Los requisitos hardware dependen tanto del sistema operativo (Windows o Linux) como del número de usuarios, operadores, equipos monitorizados. Compruebe que los requisitos hardware se adecuan al tamaño de su sistema mediante las tablas expuestas en la sección “Hardware requirements” de [REF4].
35. En cuanto a los requisitos software existen varias combinaciones posibles de sistema operativo (ej. Windows Server 2022) y bases de datos (ej. SQL Server 2022 Enterprise). Para comprobar que se dispone del software necesario, ver la sección “Software Requirements” de [REF4]).

    Nota: Revisar que no se ha alcanzado End of Life (EOL) de los sistemas operativos y bases de datos antes de utilizarlos en el sistema.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

36. En el entorno de operación de iMC MagicBox deben considerarse distintos componentes que proporcionan servicios de soporte.
    - **Estación de gestión:** Los administradores acceden al portal web desde un PC cliente con navegador compatible (Firefox, Chrome, Edge), que actúa como estación de

gestión. Ver “Accessing iMC” en [REF4], para comprobar las características del navegador.

- **Servidores de autenticación externos:** iMC UAM se integra con servidores RADIUS y LDAP para autenticar usuarios y dispositivos. Ver apartado 6.6 SERVIDORES DE AUTENTICACIÓN para más información.
- **Servidores de auditoría:** iMC permite integración con un servidor Syslog externo, para centralizar eventos y alarmas. Ver sección 6.11.3 REENVÍO DE EVENTOS para más información.
- **Dispositivos gestionados:** Los switches, routers, puntos de acceso y otros equipos de red configurados para ser gestionados por la plataforma iMC.

5 FASE DE INSTALACIÓN

37. Para llevar a cabo la instalación de iMC MagicBox se deben seguir los pasos definidos en el documento [REF4]. A continuación, mostramos los puntos más importantes y las configuraciones específicas que se deben llevar a cabo para que la instalación resulte en la configuración cualificada del producto.

5.1 PREPARACIÓN PARA LA INSTALACIÓN

38. Para preparar el entorno de instalación se deben seguir los siguientes pasos:

    - Comprobar que los requisitos Hardware y Software son compatibles con lo definido en el apartado **¡Error! No se encuentra el origen de la referencia.** 4.4 CONSIDERACIONES PREVIAS de este documento.
    - Comprobar que los puertos necesarios para el correcto funcionamiento del producto se encuentran abiertos (“Checking ports and firewalls” en [REF4]).
    - Antes de instalar iMC, asegúrate de que la base de datos (SQL Server u Oracle) y su cliente estén correctamente configurados para iniciarse automáticamente con el sistema operativo y cumplan los requisitos específicos de permisos y red (“Checking the database configuration” en [REF4]).
    - Antes de instalar iMC, se debe disponer de la contraseña de una cuenta con privilegios de superusuario en la base de datos, ya que iMC la utiliza para crear sus archivos y cuentas, y cualquier cambio posterior de esa contraseña debe actualizarse también en iMC para evitar fallos en la gestión y despliegue de componentes. Para cambiar la contraseña en iMC ver “Superuser account” en [REF4].

5.2 INSTALACIÓN

39. Para llevar a cabo la instalación hay que seguir las instrucciones que se encuentran en la sección “Installing and deploying the IMC platform” en [REF4]. En dicha sección se encuentran los pasos a seguir, comandos a ejecutar e imágenes de ejemplo.
40. La instalación consta de dos fases, una de instalación y otra de despliegue. La fase de instalación consta de dos modos distintos, instalación típica (sección “Installing the IMC platform in typical mode” en [REF4]) o instalación personalizada (sección “Installing the IMC platform in custom mode” en [REF4]).
41. Tras la instalación comienza el proceso guiado de despliegue mediante el “Intelligent Deployment Monitoring Agent”. Este proceso está descrito en la sección “Deploying the IMC platform component” en [REF4].

5.3 INSTALACIÓN DE COMPONENTES ADICIONALES

42. Los **iMC service components** son módulos opcionales que complementan la **plataforma base de iMC** para proporcionar funciones específicas de gestión de red, seguridad y servicios. Sin ellos, la plataforma solo ofrece capacidades básicas de descubrimiento y supervisión, mientras que con estos módulos se amplían las funciones (ej. control de acceso, auditoría, análisis de tráfico, VPN, Wi-Fi, etc.). Su instalación esta descrita en la sección “Installing and deploying IMC service components” de [REF4].

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

43. iMC MagicBox no tiene un comando o parámetro de configuración específico que ponga el producto en una configuración segura. Para llevar a cabo la configuración cualificada se deben seguir las configuraciones que se encuentran en los siguientes apartados.

6.2 AUTENTICACIÓN

44. En cuanto a la autenticación tenemos la autenticación de los administradores contra el iMC y la autenticación de los dispositivos gestionados.

6.2.1 AUTENTICACIÓN DE ADMINISTRADORES

45. Para acceder a la plataforma de gestión de iMC, es necesario autenticarse a través de la interfaz web del servidor. El procedimiento de inicio de sesión garantiza que únicamente los usuarios autorizados puedan acceder a las funciones de administración y supervisión del sistema.
46. Para iniciar sesión en iMC:
    a) Introduzca en el navegador la URL del servidor iMC, incluyendo el número de puerto asignado a iMC. Utilizar siempre HTTPS para realizar la conexión:
    - https://nombre_servidor:número_puerto/imc

      Donde `nombre_servidor` es el nombre del servidor iMC y `número_puerto` es el puerto TCP asignado a iMC durante la instalación. De forma alternativa, puede usarse la dirección IP del servidor en lugar del nombre del servidor.

    b) Introduzca el ID de usuario que se le haya asignado en el campo `Operator`.

    c) Introduzca su contraseña en el campo `Password`.

    d) Haga clic en Log In o presione `Enter`.

6.2.1.1 PRIMERA AUTENTICACIÓN

47. El nombre de usuario predeterminado para el administrador de iMC es `admin`.
48. Para las versiones anteriores a `IMC PLAT 7.3 (E0706)`, la contraseña predeterminada es `admin`. Para `IMC PLAT 7.3 (E0706)` y versiones posteriores, la contraseña predeterminada es `Pwd@12345`.
49. IMPORTANTE: Es necesario cambiar la contraseña de administración tras la primera autenticación. Para realizar esta operación, primero hay que configurar la política de contraseñas siguiendo el procedimiento de la sección 6.3.2.4POLÍTICA DE CONTRASEÑAS y posteriormente cambiar la contraseña como se indica en la sección 6.3.2.2MODIFICACIÓN DE CONTRASEÑAS.

6.2.2 AUTENTICACIÓN DE DISPOSITIVOS GESTIONADOS

50. iMC incluye diferentes mecanismos de autenticación que le permiten el acceso a los dispositivos gestionados, así como la protección de los datos utilizados para la administración de los mismos. A continuación, se describen las principales opciones relacionadas con la autenticación (ver sección “Securing IMC and access to managed resources” en [REF1]):

    - **Configuración SNMP:** para comunicaciones seguras entre iMC y los dispositivos gestionados, iMC admite SNMPv1, v2c y varias formas de v3, pero en su versión cualificada solo es posible utilizar SNMPv3. Además, iMC admite la gestión global de cadenas de comunidad SNMP para todos los dispositivos gestionados, una vez que estos se han configurado para ser administrados por iMC. Para configurar SNMP mediante plantillas, consulte la sección "SNMP templates" en concreto “Adding an SNMPv3 template” en [REF4].
    - **Configuración SSH:** iMC también admite el acceso remoto a dispositivos a través de Telnet (uso no permitido en versión cualificada) y SSH, con la posibilidad de utilizar plantillas para configurar sus parámetros. Para configurar estas plantillas, consulte "Device access templates" en [REF4].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

51. Es importante señalar que **no existe un modo de administración local** propiamente dicho sobre el propio producto. El acceso y gestión de la plataforma se realizan siempre de manera remota a través de la **interfaz web**. La única interacción local que se produce con el sistema es durante las fases de **instalación, desinstalación del producto y recuperación de contraseñas**, donde el administrador debe operar directamente sobre el servidor o la máquina virtual que aloja iMC, siguiendo los procedimientos descritos en [REF4].
52. En la plataforma iMC, la administración a través de HTTPS se configura desde la propia consola web. El producto permite forzar que el acceso se realice únicamente por HTTPS, deshabilitando HTTP como protocolo inseguro. Esta configuración asegura que todas las sesiones de gestión gráfica con iMC estén protegidas mediante un canal cifrado.
53. Para realizar esta configuración, el administrador debe ejecutar el siguiente procedimiento (ver “HTTPS access settings” en [REF1]):

    a) Vaya a `System > HTTPS Access Settings`.

    b) Haga clic en la pestaña `System` en la parte superior de la navegación por pestañas.

    c) Haga clic en `HTTPS Access Settings`, ubicado en la sección `System Configuration` de la página `System`.

    d) Se abrirá la página `HTTPS Access Settings`.

    e) Seleccione `enable` en la lista `Enable only HTTPS access`.

    f) Seleccione un tipo de acceso en `HTTPS Access Type`, que puede ser `Server-side Authentication` o `Mutual Authentication`.

g) Para la autenticación del lado del servidor, cargue el archivo de certificado correspondiente al servidor y establezca la contraseña asociada.

h) Para la autenticación mutua, cargue el archivo de certificado del servidor y el certificado raíz del cliente, y establezca por separado las contraseñas de cada uno.

i) Haga clic en `OK`, o en `Restore Initial Value` para reconfigurar los valores.

j) Reinicie el sistema para que la configuración tenga efecto.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

6.3.2.1 ROLES DE USUARIO Y CONTROL DE ACCESO

54. La **gestión de operadores** en iMC permite controlar de forma segura quién accede a la plataforma y a qué recursos. A través de operadores, grupos y vistas se definen permisos y restricciones que determinan qué funciones y dispositivos están disponibles para cada usuario (ver sección “Operator management: managing secure access to IMC” en [REF1]).

55. En primer lugar, iMC organiza los permisos mediante tres mecanismos:

- Los **grupos de operadores**, que definen qué funciones de la plataforma puede utilizar cada usuario (ver “Managing operator groups” en [REF1]).
- Las **vistas de dispositivos**, que agrupan equipos de forma lógica para facilitar la gestión (ver “Viewing devices with Device, IP, and Topology views” en [REF1]).
- **Grupos de dispositivos**, que permiten restringir el acceso a conjuntos concretos de equipos según su tipo o cualquier otro criterio (ver “Group Management: managing resources using groups in iMC” en [REF1]).

56. Cada operador combina estos elementos en su cuenta, lo que determina sus derechos de acceso.

57. En cuanto a los roles predeterminados, estos se diferencian de la siguiente manera (ver “Managing operator groups” en [REF1]):

- **Administradores (ADMIN)**: disponen de acceso completo a todas las funciones y recursos de iMC, incluyendo la posibilidad de crear, modificar y eliminar configuraciones, así como gestionar cuentas de otros operadores.
- **Mantenedores (Maintainers)**: cuentan con un nivel intermedio; pueden realizar tareas de operación y mantenimiento sobre los dispositivos y vistas asignados, pero no tienen privilegios totales de administración del sistema.
- **Visualizadores (Viewers)**: poseen el nivel más limitado, ya que solo pueden consultar información y generar informes, sin capacidad de realizar cambios en la configuración ni en los dispositivos.

58. De esta manera, iMC garantiza una separación clara de responsabilidades y reduce riesgos de acceso no autorizado a funciones críticas.

59. Por último, la plataforma ofrece varias tareas de administración habituales que permiten mantener organizada la gestión de operadores (ver “Managing operator groups” en [REF1]):

- Crear nuevos grupos de operadores asignándoles privilegios y permisos específicos.
- Modificar o copiar grupos de operadores según sea necesario.
- Eliminar grupos de operadores que ya no se utilicen.
- Configurar derechos de acceso a los datos de iMC, como la monitorización en tiempo real o el uso de plantillas de informes, asignando permisos de solo lectura o de lectura/escritura según convenga.

6.3.2.2 MODIFICACIÓN DE CONTRASEÑAS

60. Los operadores individuales de iMC gestionan sus propias contraseñas una vez que la cuenta de operador ha sido creada. Para cambiar su contraseña:
    a) Vaya a `System > Modify Password`.
    b) Haga clic en la pestaña `System` en la barra de navegación superior.
    c) Haga clic en `Operator Management`, en el árbol de navegación de la izquierda.
    d) Haga clic en `Modify Password` dentro de `Operator Management` en el árbol de navegación de la izquierda.
    e) Se abrirá la página `Modify Password`.
    f) Introduzca la contraseña antigua de la cuenta con la que ha iniciado sesión en el campo `Old Password`.
    g) Introduzca la nueva contraseña de la cuenta con la que ha iniciado sesión en el campo `New Password`.
    h) Vuelva a introducir la nueva contraseña de la cuenta con la que ha iniciado sesión en el campo `Confirm New Password`.
    i) Haga clic en `OK`.

6.3.2.3 RECUPERACIÓN DE CONTRASEÑAS

61. Esta sección describe el procedimiento para recuperar o restablecer la contraseña del usuario administrador en H3C iMC MagicBox. Este proceso debe ser realizado por personal autorizado con acceso físico o de consola al servidor (en caso de no ser un appliance físico) sobre el que se ejecuta MagicBox. Una vez completada la recuperación, se recomienda aplicar inmediatamente las medidas de seguridad indicadas para evitar riesgos de compromiso del sistema.
62. Seguir los pasos a continuación si el administrador ha extraviado la contraseña y es necesario recuperar el control del equipo:
    a) Acceda al equipo utilizando la **consola local** del servidor.
    b) Acceda al directorio donde se encuentran los binarios del cliente iMC ejecutando el siguiente comando (Si iMC se instaló en una ubicación personalizada, ajuste el directorio en consecuencia):

```
cd /opt/iMC/client/bin
```

    c) Ejecute el script de recuperación de contraseña con el siguiente comando:

```
./resetpwd.sh
```

d) Una vez completado el proceso, las credenciales del administrador se restablecen a los valores por defecto:

```
Usuario: admin
Contraseña: Pwd@12345
```

63. Después de iniciar sesión correctamente, **cambie la contraseña por defecto de forma inmediata** para prevenir riesgos de seguridad y accesos no autorizados.

6.3.2.4 POLÍTICA DE CONTRASEÑAS

64. iMC permite definir de forma global políticas de contraseñas cuando se utilizan contraseñas locales de iMC para autenticar a los operadores. Con la función de estrategia de contraseñas es posible aplicar requisitos de longitud mínima, complejidad y caducidad a todas las contraseñas de manera global. Una vez configuradas, estas estrategias se aplican inmediatamente a todas las cuentas de operador que se creen en iMC a partir de ese momento.

65. Las cuentas ya creadas mantendrán la política anterior de contraseñas hasta que los usuarios actualicen su contraseña. Un usuario administrador puede forzar el cambio de contraseña de un usuario en la siguiente autenticación como se indica en la sección "Querying and maintaining accounts in batches" de [REF2].

66. IMPORTANTE: Las políticas de caducidad no se aplican a la cuenta de Administrador de iMC creada durante la instalación. La contraseña de este administrador nunca caduca, por lo que será necesario implantar políticas procedimentales de actualización periódica de dicha contraseña para mantener la seguridad.

67. Para configurar la política de contraseñas (ver "Configuring a password strategy" en [REF1]):

    a) Vaya a `System > Password Strategy`.

    b) Haga clic en la pestaña `System` en la parte superior de la navegación por pestañas.

    c) Haga clic en `Operator Management` en el árbol de navegación de la izquierda.

    d) Haga clic en `Password Strategy` dentro de `Operator Management`.

    e) Se abrirá la página `Configure Password Strategy`.

    f) Introduzca la siguiente información en la página de configuración:

    g) Seleccione 14 como longitud mínima de la contraseña en la lista `Min. Length`.

    h) Seleccione la estrategia de complejidad "`Must Contain Letters, Numbers, and Special Characters`"en la lista `Complexity`.

    i) Seleccione el periodo de validez de las contraseñas "`60 días`" en la lista `Validity Period`.

6.3.2.5 CONFIGURACIÓN DE PARÁMETROS DE SESIÓN

68. El objetivo de esta configuración es reforzar la seguridad de acceso de los operadores en iMC. Para ello se ajustarán los parámetros de sesión de forma que se limite el tiempo de

inactividad permitido, se restrinja el número de intentos fallidos de autenticación y se establezca un tiempo de bloqueo automático tras dichos intentos. Estas opciones se configuran desde el apartado de `System Settings`, disponible en la pestaña `System`, dentro de la sección `System Configuration` (ver "System settings" en [REF1]).

69. Con este procedimiento, iMC garantiza que las cuentas de operador se cierren rápidamente si permanecen inactivas, que se proteja contra intentos de fuerza bruta en el login y que exista un periodo de bloqueo que reduzca riesgos de accesos indebidos:

    a) Haz clic en la pestaña `System` en la barra superior.

    b) En la sección `System Configuration`, selecciona `System Settings`.

    c) Se abrirá la página `System Settings`.

    d) En el campo `Operator Idle Timeout`, introduce el valor 5.

    e) En el campo `Lock Duration for Three Continuous Login Failures (1-1440 Minutes)`, introduce el valor 5.

70. Tras aplicar esta configuración:

    - Las sesiones inactivas se cerrarán a los 5 minutos.
    - Un usuario que falle tres veces seguidas al iniciar sesión quedará bloqueado automáticamente durante 5 minutos.

6.3.2.6 CONFIGURACIÓN DE MENSAJE DE INICIO DE SESIÓN

71. Un acuerdo de usuario en la página de inicio de sesión de iMC informa a los operadores sobre los derechos y obligaciones para un inicio de sesión en iMC. Para iniciar sesión en iMC, los operadores deben aceptar los términos del acuerdo de usuario.

72. Para mostrar un acuerdo de usuario en la página de inicio de sesión de iMC:

    a) En el servidor de iMC, accede al directorio `\client\conf` de la ruta de instalación de iMC (`/client/conf` en Linux).

    b) Utiliza Notepad (o vi en Linux) para abrir el archivo `commonCfg.properties`.

    c) Cambia el valor del parámetro `enableTerms` a `true`.

    d) Guarda y cierra el archivo `commonCfg.properties`.

    e) Prepara un acuerdo de usuario en formato HTML con el nombre `terms.html`.

    f) Guarda el archivo `terms.html` en el directorio `\client\web\apps\imc` de la ruta de instalación de iMC `(/client/web/apps/imc` en Linux) en el servidor de iMC.

73. Se visualizará un enlace al acuerdo de usuario, como se muestra en Ilustración 1. Los operadores pueden hacer clic en el enlace para ver los términos del acuerdo de usuario.

Ilustración 1. mensaje de inicio de sesión

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

74. Configurar los puertos y firewall del servidor de forma que el puerto HTTPS (por defecto para iMC es el puerto 8443) esté disponible desde los equipos de los administradores y operadores.
75. Este puerto por defecto se puede cambiar durante la instalación, donde el asistente solicita explícitamente configurar los puertos del servicio web en la ventana `Configure Web Service Port`.
76. Si iMC ya está instalado, puedes actualizar el puerto HTTPS a través de la opción `System > HTTPS Access Settings` en la interfaz web.
77. Dependiendo de los dispositivos gestionados y servicios configurados se deberán abrir los puertos necesarios para la comunicación de estos.
78. Cualquier otro puerto no usado deberá ser bloqueado por el sistema operativo o un elemento de red externo.

6.5 GESTIÓN DE CERTIFICADOS

79. En este apartado se describen los pasos necesarios para la generación, habilitación y utilización de clave asimétrica para la conexión SSH.
80. Para realizar la configuración de certificados para el iMC seguir los siguientes pasos:
    a) Generar un par de claves utilizando `ssh-keygen` en el iMC. Ejecute el siguiente comando:

```
ssh-keygen -t rsa
```

b) Seguir el asistente interactivo: se puede elegir la ubicación predeterminada para generar la clave y el nombre del archivo, así como establecer una contraseña. En la Ilustración 2, se generan los archivos `id_rsa` que es la clave privada y `id_rsa.pub` que es la clave pública:

```
[root@matrix01 ~]# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:02VtGdwXJ+sW74tTLByHfXXQ5cR9X5mju1SafRhf8ZI root@matrix01
The key's randomart image is:
+---[RSA 3072]----+
|              o=O|
|            . . X@|
|             o B.%|
|            . BEB=|
|         S o = %=+|
|          + . O.=o|
|         o   . + o|
|          .    o. .|
|               ... |
+----[SHA256]-----+
```

Ilustración 2. Ejemplo de uso del asistente

c) Habilitar la clave generada. Pedirá la contraseña de la cuenta del administrador del sistema operativo donde esté instalado el producto, en el ejemplo se ha representado este usuario como “root”:

```
ssh-copy-id root@server-ip
```

d) Reiniciar el servicio ssh

```
systemctl restart sshd
```

e) Copie el archivo de clave pública al equipo local.

f) Inicie sesión en iMC y vaya a `System > Resource Management > Access Parameter Template > SSH`.

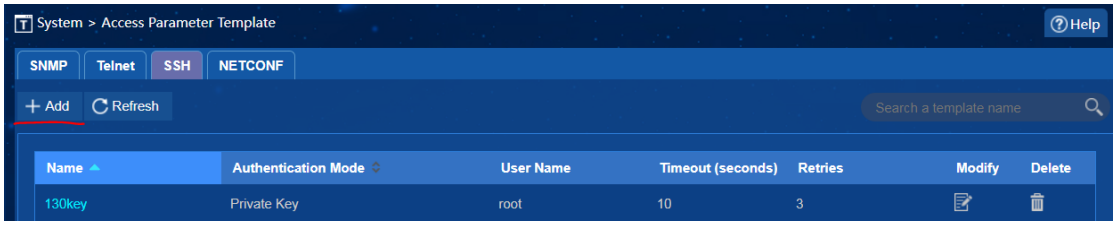

Ilustración 3. SSH Template

g) Cree una plantilla SSH, seleccione “Private Key” como método de autenticación, introduzca root como nombre de usuario, seleccione el archivo de clave privada generado en el paso “b)”.

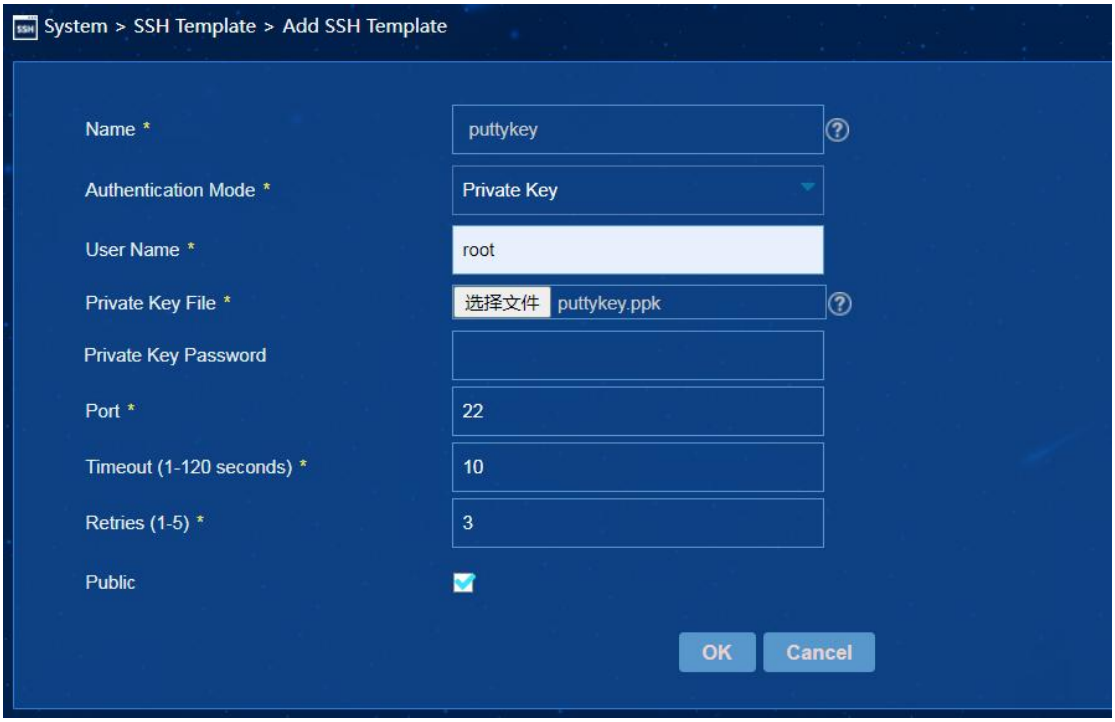

Ilustración 4. Configuración SSH Template

h) haga clic en `OK`.

6.6 SERVIDORES DE AUTENTICACIÓN

81. Para reforzar la seguridad del acceso a IMC y permitir una gestión unificada de nombres de usuario y contraseñas, iMC admite el uso de servicios de autenticación de inicio de sesión con RADIUS, LDAP y TACACS (ver sección "Securing IMC access through authentication services" en [REF1]).

82. Solo los administradores u operadores que sean miembros de un grupo con nivel de privilegio ADMIN pueden configurar los servicios de autenticación.

6.6.1 CONFIGURACIÓN CON RADIUS

83. Para una configuración segura de RADIUS en iMC, se recomienda utilizar CHAP en lugar de PAP para evitar el envío de credenciales en texto claro, definir un secreto compartido largo, aleatorio y complejo y proteger las comunicaciones entre iMC y el servidor RADIUS mediante un canal cifrado, encapsulando el tráfico RADIUS en un túnel seguro (IPsec/VPN). Si no se cumplen con estos requisitos se recomienda utilizar otro tipo de servidor de autenticación.

84. Para configurar un servidor de autenticación de tipo RADIUS seguir los siguientes pasos:

    a) Vaya a `System > AuthenticationServer`.

    b) Haga clic en la pestaña `System` de la barra de navegación superior.

    c) Haga clic en `Operator Management` en el árbol de navegación de la izquierda.

d) Haga clic en `Authentication Server` dentro de `Operator Management` en el árbol de navegación de la izquierda. Se abrirá la página de configuración del servidor de autenticación.

e) En el área `RADIUS Server`, configure los siguientes parámetros:

- **Authentication Type:** Seleccione el tipo de autenticación CHAP, en la lista desplegable. Esta elección debe coincidir con el tipo de autenticación configurado en el servidor RADIUS.
- **Primary Server:** Introduzca la dirección IP o el nombre de host del servidor RADIUS principal.
- **Secondary Server:** Introduzca la dirección IP o el nombre de host del servidor RADIUS secundario.
- **Authentication Port:** Introduzca el número de puerto que utiliza el servidor RADIUS para la autenticación. El valor por defecto es 1812.
- **Shared Secret:** Introduzca la clave compartida para los paquetes de autenticación. Lo configurado aquí debe coincidir con lo configurado en el servidor RADIUS.
- **Advanced Settings:** Haga clic en `Advanced Settings` y luego configure si desea habilitar la función `Synchronize Radius Operator` en el cuadro de diálogo que se abre.
  - Para habilitar la función `Synchronize Radius Operator`, selecciónela. Introduzca el `Vendor ID` y el `Vendor type` del servidor RADIUS, configure el tipo de dato y el valor de los contenidos de coincidencia, seleccione un grupo de operadores de la lista `Operator Group` y haga clic en `Add Match Rule` para añadir reglas de coincidencia. Si el operador no existe, pero pasa la autenticación RADIUS y las reglas coinciden, el sistema guarda la información del operador en el grupo de operadores.
  - Para deshabilitar esta función, desmarque `Synchronize Radius Operator`.

f) Haga clic en `OK`.

6.6.2 CONFIGURACIÓN CON LDAP

85. Se recomienda configurar siempre LDAPv3 junto con una conexión segura mediante TLS/SSL (LDAPS), ya que LDAPv2 está obsoleto y no ofrece mecanismos de protección adecuados. El uso de LDAPv3 con TLS garantiza el cifrado de las credenciales y de la información transmitida, reforzando la seguridad frente a ataques de interceptación o manipulación de datos.
86. Para configurar un servidor de autenticación de tipo LDAP seguir los siguientes pasos:

a) Vaya a `System > AuthenticationServer`.

b) Haga clic en la pestaña `System` de la barra de navegación superior.

c) Haga clic en `Operator Management` en el árbol de navegación de la izquierda.

d) Haga clic en `Authentication Server` dentro de `Operator Management` en el árbol de navegación de la izquierda. Se abrirá la página de configuración del servidor de autenticación.

e) En el área `LDAP Server`, configure los siguientes parámetros:

- **LDAP Version**: Seleccione la versión de LDAP 3, de la lista. La opción seleccionada debe coincidir con la configuración del servidor LDAP.
- **Server Type**: Seleccione el tipo de servidor LDAP de la lista. iMC admite Generic LDAP Services así como Microsoft Active Directory.
- **Server Address**: Introduzca la dirección IP o el nombre de host del servidor LDAP en el campo correspondiente.
- **Server Port**: Introduzca el número de puerto que usa el servidor LDAP para autenticación. El puerto por defecto es 389.
- **Base DN**: Introduzca el valor de Base DN que se usará para la comunicación con el servidor LDAP. Debe coincidir con lo configurado en el servidor de autenticación LDAP.
- **Admin DN**: Introduzca el valor de Admin DN que se usará para la comunicación con el servidor LDAP. Debe coincidir con lo configurado en el servidor de autenticación LDAP.
- **Admin Password**: Introduzca la contraseña del administrador para la comunicación con el servidor LDAP. Debe coincidir con lo configurado en el servidor de autenticación LDAP.
- **Username Attribute**: Introduzca el atributo de nombre de usuario que se usará para obtener información de usuarios desde el servidor LDAP. Debe coincidir con lo configurado en el servidor de autenticación LDAP.
- **Advanced Settings**: Haga clic en `Advanced Settings`, y luego configure si desea habilitar la función `Synchronize LDAP Operator` en el cuadro de diálogo que se abre.
  - Para habilitar la función `Synchronize LDAP Operator`, seleccione `Synchronize LDAP Operator`. Introduzca una **OU** en el campo correspondiente, seleccione un grupo de operadores de la lista `Operator Group` y haga clic en `Add Match Rule` para añadir reglas de coincidencia. Si el operador no existe, pero pasa la autenticación LDAP y las reglas coinciden, el sistema guarda la información del operador en el grupo de operadores.
  - **OU**: Parte de la entrada de usuario en LDAP que identifica el grupo de operadores del usuario en el servidor LDAP.
  - **Operator Group**: Grupo de operadores en el sistema que coincide con la OU.
  - **Operation**: Permite definir derechos de acceso a grupos de usuarios, grupos de dispositivos y vistas personalizadas para un operador sincronizado. Los operadores sincronizados y los añadidos manualmente usan el mismo método para definir derechos de acceso. Un operador sincronizado será eliminado cuando se borre la regla de sincronización.
- Para deshabilitar la función `Synchronize LDAP Operator`, desmarque la opción.
- **Require Security Connection (SSL)**: Especifica si se debe usar una conexión segura **SSL** para conectarse al servidor LDAP. Esta opción debe estar siempre marcada.

6.6.3 CONFIGURACIÓN CON TACACS

87. Para configurar un servidor de autenticación de tipo TACACS seguir los siguientes pasos:

    a) Vaya a `System > AuthenticationServer`.

    b) Haga clic en la pestaña `System` de la barra de navegación superior.

    c) Haga clic en `Operator Management` en el árbol de navegación de la izquierda.

    d) Haga clic en `Authentication Server` dentro de `Operator Management` en el árbol de navegación de la izquierda. Se abrirá la página de configuración del servidor de autenticación.

    e) En el área `TACACS Server`, configure los siguientes parámetros:

- **Authentication Type**: Seleccione un tipo de autenticación TACACS. Las opciones son ASCII, PAP y CHAP.
- **TACACS Server**: Introduzca la dirección IP o el nombre de host del servidor TACACS.
- **Authentication Port**: Introduzca el número de puerto de autenticación del servidor TACACS. El valor por defecto es 49.
- **Shared Secret**: Introduzca la clave compartida para la autenticación de identidad. Debe ser la misma que la configurada en el servidor TACACS.

    f) Haga clic en `OK`.

6.7 SINCRONIZACIÓN

88. La sincronización horaria en la plataforma iMC es un requisito fundamental para garantizar la integridad de los registros, la coherencia en los eventos de auditoría y la validez de las comunicaciones seguras entre componentes.
89. El producto permite al administrador realizar el ajuste de la hora del sistema. Para realizar esto se requiere realizar una conexión a través de línea de comandos (CLI). Una vez que se accede a la línea de comandos se puede establecer la fecha y hora con los siguientes comandos:

    a) Establecer fecha y hora manualmente (formato: MMDDhhmmYYYY).

```
sudo date MMDDhhmmYYYY
```

    b) Mostrar la fecha y hora para comprobar que el comando se ejecutó correctamente:

```
Date
```

    c) Sincronizar la hora del sistema con la del hardware

```
sudo hwclock --systohc
```

6.7.1 CONFIGURACIÓN NTP

90. Esta sección describe el procedimiento para configurar la sincronización horaria mediante NTP (Network Time Protocol) en H3C iMC MagicBox. Mantener la hora del sistema

correctamente sincronizada es esencial para el correcto funcionamiento del equipo (ej. análisis de logs).

91. La configuración de la sincronización horaria mediante NTP se debe seguir el siguiente procedimiento:

    a) Inicie sesión en el sistema utilizando una cuenta de administración.

    b) Abra el fichero de configuración de NTP con el siguiente comando:

```
sudo vi /etc/ntp.conf
```

    c) En el fichero de configuración, añada o modifique las siguientes líneas para definir el/los servidor(es) NTP:

```
server <IP_O_HOSTNAME_NTP> iburst
```

    d) Compruebe la zona horaria actual del sistema:

```
Timedatectl
```

    e) Si es necesario, configure la zona horaria correcta:

```
sudo timedatectl set-timezone <location>
```

    f) Inicie el servicio NTP:

```
sudo systemctl start ntpd
```

    g) Configure el servicio para que se inicie automáticamente tras un reinicio del sistema:

```
sudo systemctl enable ntpd
```

    h) Compruebe que el servicio NTP se encuentra en ejecución correctamente:

```
sudo systemctl status ntpd
```

    i) Tras unos minutos, verifique que el sistema se ha sincronizado con los servidores NTP configurados. Si la sincronización es correcta, los servidores NTP remotos aparecerán listados con estado alcanzable:

```
ntpq -p
```

    j) Si el cortafuegos del sistema está activo, permita el tráfico NTP:

```
sudo firewall-cmd --add-service=ntp --permanent
sudo firewall-cmd –reload
```

92. La opción `iburst` (apartado “c)”) permite una sincronización inicial más rápida al acelerar el intercambio inicial de paquetes con los servidores NTP. Asimismo, se recomienda configurar **al menos dos servidores NTP** con el fin de proporcionar redundancia y mejorar la disponibilidad y fiabilidad de la sincronización horaria.

6.8 ACTUALIZACIONES

93. El proceso de actualización de iMC MagicBox está descrito en la sección “Upgrading the IMC platform” de [REF4] .

94. Antes de realizar la actualización hay que seguir los siguientes pasos:

a) Obtenga los paquetes de actualización para la plataforma iMC y para todos los componentes de servicio desplegados. Recuerde que después de actualizar la plataforma iMC, debe actualizar todos los componentes de servicio para que coincidan con la nueva versión de la plataforma iMC.

b) Planifique una ventana de mantenimiento para minimizar impacto en el sistema.

c) Realice una copia de seguridad de los archivos de la base de datos de iMC utilizando la función de copia de seguridad manual de DBMan (ver sección 6.12 BACKUP). Detenga todos los procesos de iMC y, a continuación, guarde el directorio de instalación de iMC en una ruta de respaldo. Si la actualización falla, podrá utilizar estos archivos para restaurar iMC.

95. Para descargar el paquete de instalación de H3C iMC se usará el portal de soporte de H3C y se debe tener una cuenta con permisos (cliente final o partner). El portal de descarga se encuentra en https://www.h3c.com/en/Support/Resource_Center/Software_Download/.

96. Ejecute el proceso de instalación:

a) Inicie el `Intelligent Deployment Monitoring Agent` en el servidor y, a continuación, haga clic en `Install` en la pestaña Monitor.

b) Se abrirá el cuadro de diálogo `Choose folder`, como se muestra en la Ilustración 5.

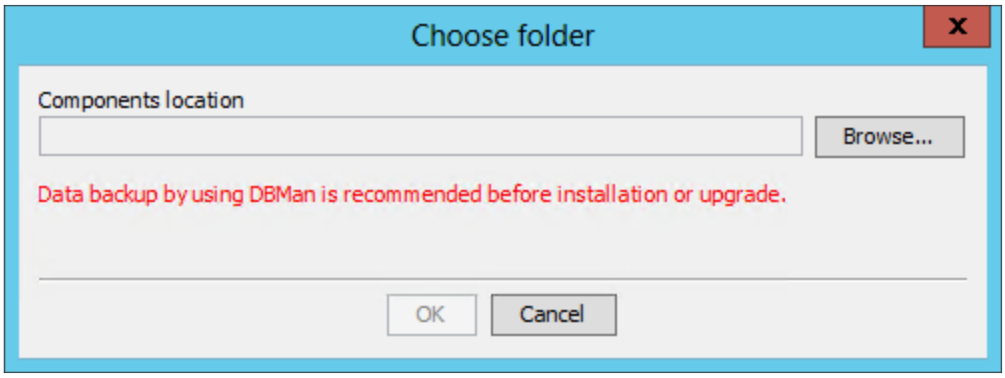

Ilustración 5. Dialogo "Choose folder"

c) Continúe con los pasos como se indican en la sección “Upgrading the IMC platform” de [REF4].

6.9 AUTO-CHEQUEOS

97. Durante el arranque del TOE, éste primero verifica la integridad del firmware y, a continuación, ejecuta una serie de pruebas para garantizar que sus funciones criptográficas se ejecutan correctamente. Si alguna de estas comprobaciones falla, el dispositivo se detendrá y requerirá la intervención del administrador para poder iniciar correctamente.

6.10 ALTA DISPONIBILIDAD

98. En una implementación distribuida de H3C iMC (Intelligent Management Center), el sistema se organiza en torno a dos tipos de servidores: conductor y miembro.

99. El servidor conductor actúa como núcleo central de la plataforma. Es el punto de acceso principal para los administradores, ya que ofrece un portal web unificado desde el que se gestionan todos los recursos y componentes del sistema. Además, es el responsable de coordinar la instalación, despliegue y control de los servicios que se ejecutan en el resto de servidores. Todos los componentes de la plataforma se instalan inicialmente en el conductor, y desde él se distribuyen a los servidores miembro que correspondan.

100. Los servidores miembro se encargan de ejecutar tareas específicas asignadas por el conductor. Por ejemplo, pueden albergar funciones de análisis de tráfico (NTA) o servicios de autenticación de usuarios (Portal de UAM). Estos servidores trabajan siempre bajo la dirección del conductor, que mantiene la lógica de coordinación y centralización. Los usuarios acceden siempre al portal del conductor, y este se encarga de redirigir y orquestar las operaciones que requieran la participación de los miembros.

101. Es importante destacar que el esquema conductor-miembro de iMC no proporciona un mecanismo de *failover* automático. Si un servidor miembro deja de estar disponible, las funciones que este ejecutaba quedan interrumpidas hasta que el servicio se restaure. De igual manera, la caída del servidor conductor provoca la pérdida del portal de gestión y de la coordinación central. Para lograr redundancia real y tolerancia a fallos, iMC requiere la utilización de componentes adicionales, como la herramienta iHA Tool, que permite implementar clústeres de alta disponibilidad.

    NOTA: Para más información sobre las opciones de despliegue consultar las secciones “Deployment restrictions and guidelines” y “Deploying IMC on a member server (distributed deployment)” de [REF4].

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

102. El componente principal para auditar las actividades internas de los operadores es la función de Registros de Operación (Operation Log). Estos archivos de registro detallan los eventos generados por el sistema.

103. El listado de Registros de Operación (Operation Log list) muestra la siguiente información para rastrear la actividad:

- **Operador (Operator):** Contiene el nombre del usuario que ejecuta la operación.
- **Dirección IP (IP Address):** Contiene la dirección IP del operador que ejecuta la operación documentada.
- **Nombre del Módulo (Module Name):** Contiene el nombre del módulo de iMC que generó la entrada de registro.
- **Operación (Operation):** Contiene una descripción de la operación, acción o resultado.

104. Para configurar el registro de eventos local seguir los pasos indicados en la sección “Log configuration” de [REF1].

6.11.2 ALMACENAMIENTO LOCAL

105. iMC escribe información de auditoría a nivel de sistema y de operador en archivos de registro. Uno de estos archivos es el registro de operaciones, que contiene información sobre la actividad de los operadores de iMC (ver sección “Log files” en [REF1]).

106. Para ver los registros de auditoría ir a “System > Operation Log”. Si tiene varias páginas, utilizar los botones “<<”, “<”, “>”, “>>” para ver las distintas páginas. Para configurar el número de entradas a ver por página, utilizar los botones “8”, “15”, “50”, “100” o “200”.

6.11.3 REENVÍO DE EVENTOS

107. El sistema H3C Intelligent Management Center (iMC) permite exportar los registros de operación (operation logs) a un servidor Syslog remoto. Esta configuración facilita la centralización y el análisis de eventos relacionados con la administración del propio iMC (acciones de operadores, cambios de configuración, accesos, etc.), mejorando la trazabilidad y la seguridad del entorno.

108. Para realizar la configuración para enviar los registros de auditoría a un servidor (syslog) seguir el siguiente procedimiento como administrador:

a) En la parte superior, seleccione la pestaña `System`.

b) En el menú lateral, vaya a `System Configuration → System Settings`.

c) En la página `System Settings`, desplácese hasta la sección `Forwarding IMC operation logs in syslogs`.

d) En el campo `Enable Forwarding of IMC Operation Logs in Syslogs`, seleccione `Yes` para habilitar la exportación.

e) En el campo `Syslog Server IP`, introduzca la dirección IP del servidor Syslog de destino.

f) En el campo `Syslog Server Port`, introduzca el puerto de recepción del servidor.

g) Haga clic en `OK` para aplicar la configuración.

6.12 BACKUP

109. DBMan es la herramienta de copia de seguridad y restauración automática para las bases de datos de la plataforma iMC y de sus componentes de servicio, y proporciona una solución completa de respaldo ante desastres del sistema. DBMan utiliza un mecanismo estándar de copia de seguridad y restauración SQL para procesar las bases de datos completas.

110. DBMan admite tanto copias de seguridad y restauraciones manuales como automáticas. Está integrado en la pestaña `Environment` del `Intelligent Deployment Monitoring Agent`, como se muestra en la Ilustración 6.

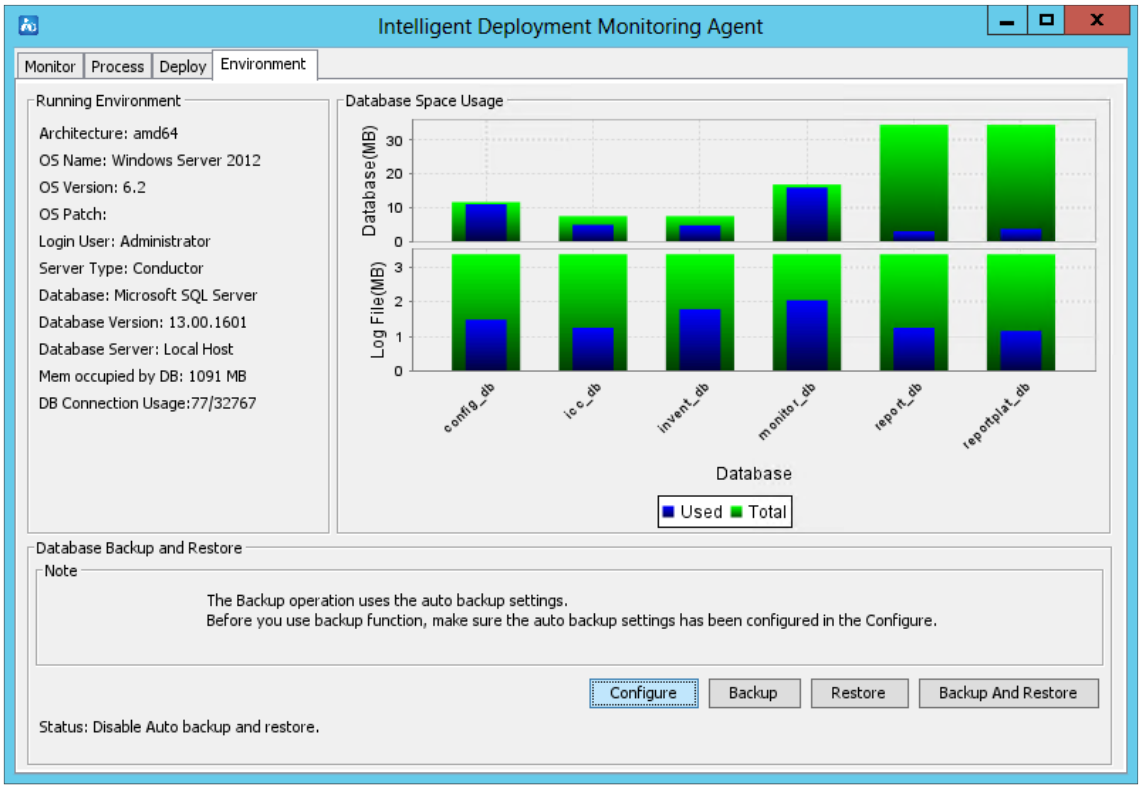

Ilustración 6. Pestaña Environment

111. La pestaña `Environment` incluye las siguientes áreas:

- **Running Environment**: muestra la información de software y hardware del servidor iMC.
- **Database Space Usage**: muestra la información de uso de la base de datos y de los archivos de registro de cada componente en el servidor iMC.
- **Database Backup and Restore**: proporciona las siguientes opciones de copia de seguridad y restauración de bases de datos:
  - **Configure**: permite configurar los parámetros de copia de seguridad y restauración automática de la base de datos. Esta función se utiliza normalmente en escenarios de conmutación por error sin estado (*stateless failover*).
  - **Backup**: realiza de inmediato una copia de seguridad de todos los archivos de datos de iMC (incluidos los archivos de configuración y de base de datos) en una ruta especificada.
  - **Restore**: restaura de inmediato en el servidor iMC los archivos de base de datos previamente respaldados.
  - **Backup And Restore**: realiza de inmediato una copia de seguridad de la base de datos en el servidor principal hacia el servidor de respaldo y efectúa la restauración automática. Esta opción es aplicable a escenarios de conmutación por error sin estado (*stateless failover*).

112. Para más información, ver la sección “Backing up and restoring the database” en [REF4].

7 REFERENCIAS

113. A continuación, se indica la documentación que se ha referenciado a lo largo de la guía y que será facilitada por el proveedor.

[REF1] H3C Intelligent Management Center, Enterprise and Standard Platform, Administration Guide, v. 5W112-20190716

https://www.h3c.com/en/Support/Resource_Center/EN/Network_Management/Catalog/H3C_IMC/IMC/Technical_Documents/Configure___Deploy/User_Manuals/H3C_IMC_Enterprise_Standard_Platform-7.3-5W112/

[REF2] H3C Intelligent Management Center, User Access Manager, Administrator Guide, v. 5W108-20210331

https://www.h3c.com/en/Support/Resource_Center/EN/Network_Management/Catalog/H3C_IMC/IMC/Technical_Documents/Configure___Deploy/User_Manuals/H3C_IMC_UG/

[REF3] H3C Intelligent Management Center, TACACS+ Authentication Manager, Administrator Guide, v. 5W106-20190730

https://www.h3c.com/en/Support/Resource_Center/HK/Network_Management/H3C_IMC_DC/IMC/Technical_Documents/Configure___Deploy/User_Manuals/H3C_TACACS+Authentication_Manager_AG-7.3-5W106/

[REF4] H3C Intelligent Management Center, Deployment Guide v. 5W100-20241218

https://www.h3c.com/en/Support/Resource_Center/EN/Network_Management/Catalog/H3C_IMC/IMC/Technical_Documents/Install___Upgrade/Installation_Guides/H3C_IMC_Deploy-23881/01/

[REF5] H3C Software Products Remote Licensing Guide, v. 5W102-20230707

https://www.h3c.com/en/Support/Resource_Center/EN/Home/Public/00-Public/Technical_Documents/Install___Upgrade/Licensing_Guides/Software_Products_Remote_Licensing-Long/

8 ABREVIATURAS

ADMIN	Administrator
ASCII	American Standard Code for Information Interchange
CHAP	Challenge Handshake Authentication Protocol
CPSTIC	Catálogo de Productos y Servicios de Tecnologías de la Información y las Comunicaciones
DBMan	Database Manager
DN	Distinguished Name
EAD	Endpoint Admission Defense
EIA	Enterprise Intelligent Access
ENS	Esquema Nacional de Seguridad.
EOL	End of Life
H3C	Huasan ThreeCom
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identification
IE	Internet Explorer
iHA	Intelligent High Availability
iMC	Intelligent Management Center
IP	Internet Protocol
IPsec	Internet Protocol Security
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol Secure
LDAPv2	Lightweight Directory Access Protocol Version 2
LDAPv3	Lightweight Directory Access Protocol Version 3
MC	Management Center
NTA	Network Traffic Analyzer
OK	Okay
OU	Organizational Unit
PAP	Password Authentication Protocol
PC	Personal Computer
RADIUS	Remote Authentication Dial-In User Service
SNMP	Simple Network Management Protocol

SNMPv1	Simple Network Management Protocol version 1
SNMPv3	Simple Network Management Protocol version 3
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
Syslog	System Log
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
UAM	User Access Manager
URL	Uniform Resource Locator
v2c	version 2 community
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity